Explicit Frames for Deterministic Phase Retrieval via PhaseLift

Michael Kech[1,*]

[1]*Department of Mathematics, Technische Universität München, 85748 Garching, Germany*

(Dated: January 24, 2017)

We explicitly give a frame of cardinality $5n-6$ such that every signal in $\mathbb{C}^n$ can be recovered up to a phase from its associated intensity measurements via the PhaseLift approach. Furthermore, we give explicit linear measurements with $4r(n-r)+n-2r$ outcomes that enable the recovery of every positive semidefinite $n \times n$ matrix of rank at most r.

Keywords: phase retrieval, PhaseLift, low-rank matrix recovery, quantum state tomography

Contents

I. INTRODUCTION AND MAIN RESULT

Phase Retrieval is the task of reconstructing a signal $x \in \mathbb{C}^n$ up to a phase from intensity measurements.

In [1] it was shown that $m \geq 4n-2$ generic intensity measurements suffice to discriminate any two signals in $\mathbb{C}^n$ up to a phase. With a similar approach this result was slightly improved to $m \geq 4n-4$ in [2] [1]. The bound $m \geq 4n-4$ is known to be close to optimal. More precisely, by relating phase retrieval to the problem of embedding complex projective space in Euclidean space, it was shown in [6] that, up to terms at most logarithmic in n, $m \geq 4n-4$ intensity measurements are necessary to discriminate any two signals in

*Electronic address: kech@ma.tum.de

[1] In the context of pure state tomography, [3–5] show that the $4n-4$ bound also holds for von Neumann measurements. In addition similar bounds for the recovery of low-rank matrices with constrained measurements are provided in [3].

$\mathbb{C}^n$ up to a phase. However, [1, 2] do not provide a tractable recovery scheme. A result indicating that some redundancy is needed in order to allow for computationally efficient phase retrieval is given in [7].

There have been several approaches that do provide recovery schemes [8–10], in the present paper however we focus on the approach of [11] known as PhaseLift. Their approach consists of two steps: First, phase retrieval is lifted to the problem of recovering rank one Hermitian matrices from linear measurements. Secondly, by means of a convex relaxation, the recovery problem is formulated as a trace norm minimization over a spectrahedron. The authors of [11] then prove that $\mathcal{O}(n)$ intensity measurements suffice to recover a signal modulo phase with high probability by solving the relaxed optimization problem. Furthermore, stability guarantees for the recovery were established in [12, 13]. While these convex relaxations are in principal tractable, solving them becomes computationally expensive with increasing signal dimension [14].

However, [11–13] still leave room for improvement. For example, by working with Gaussian random vectors additional structure that might facilitate the use of PhaseLift is not incorporated and also from a practical point of view Gaussian random vectors might not be desirable. Recently, it was shown that a partial derandomization of PhaseLift can be achieved by using spherical designs [15, 16]. The purpose of the present paper is similar. However, rather than drawing the measurements from a smaller, possibly better structured set, we aim for finding explicit measurements that allow for phase retrieval via PhaseLift. Another deterministic approach to the phase retrieval problem was introduced in [17]. They improved their results in [18], providing recovery algorithms together with explicit error bounds for phase retrieval with $6n-3$ frame vectors.

Our contribution is the following: We explicitly give $5n-6$ intensity measurements from which every signal in $\mathbb{C}^n$ can be reconstructed up to a phase using PhaseLift. More precisely, for $k \in \{1,\dots,2n-3\}$ let

$$v_k := \left(1,\ x_k\, e^{\frac{i\pi}{2n}},\ x_k^2\, e^{2\frac{i\pi}{2n}},\ \dots,\ x_k^{n-1}\, e^{(n-1)\frac{i\pi}{2n}}\right)^t,\ x_k \in \mathbb{R}\setminus\{0\}. \tag{1}$$

Furthermore denote by $\{e_i\}_{i\in\{0,\dots,n-1\}}$ the standard orthonormal basis of $\mathbb{C}^n$.

Theorem I.1. *If $x_1 < x_2 < \ldots < x_{2n-3}$, then every signal $x \in \mathbb{C}^n$ can be reconstructed up to a phase from the $5n-6$ intensities*

$$\{|\langle e_0, x\rangle|^2, \dots, |\langle e_{n-1}, x\rangle|^2, |\langle v_1, x\rangle|^2, |\langle \overline{v}_1, x\rangle|^2, \dots, |\langle v_{2n-3}, x\rangle|^2, |\langle \overline{v}_{2n-3}, x\rangle|^2\}$$

via PhaseLift.

This result is stated more carefully in Section III as Corollary III.2. Its proof relies on the results of [19].

Let us highlight three features of this result:

1. To our knowledge the $5n-6$ is the smallest number of intensity measurements that allow for a uniform and computationally tractable recovery.

2. Results based on random intensity measurements typically guarantee that the recovery succeeds with high probability if the number of measurements exceeds a given

threshold which is usually determined up to a multiplicative constant. As opposed to this, Theorem I.1 comes with two advantages that might be desirable from a practical point of view: First, the recovery is not just guaranteed to succeed with high probability but indeed works deterministically. Secondly, since the measurements are given explicitly there is no need for finding a suitable value for the threshold.

3. Theorem I.1 merely requires $5n - 6$ intensity measurements. This illustrates that n additional measurements as compared to the nearly optimal bound of [1] suffice to render PhaseLift feasible.

The approach we take originates from low-rank matrix recovery [20–24] and indeed the previous results can be generalised to this setting: In Section III, we give an explicit family of linear measurements with $4r(n-r)+n-2r$ outcomes from which every positive $n \times n$ matrix of rank at most r can be recovered by means of a semidefinite program. This strongly relies on the construction of the null spaces of such measurements given in [19]. Our contribution is to explicitly characterize the orthogonal complements of these null spaces leading to the proofs of our main results.

Finally we also prove a weak stability result in Section IV, showing that the reconstruction error is linear in the error scale. As we do not know how to estimate the constant of proportionality appearing in the stability bound, this result is not of practical relevance, but might give a roadmap for proving stability in the future. However, we provide some numerical results that might indicate the constant's qualitative behaviour.

II. PRELIMINARIES

Let us first fix some notation. By $M(n,q)$ ($M(n,q,\mathbb{R})$) we denote the set of complex (real) $n \times q$ matrices. The transpose (conjugate transpose) of a matrix $A \in M(n,q)$ is denoted by A^t (A^*). For $i \in \{0,\dots,n-1\}$, $j \in \{0,\dots,q-1\}$, we denote the entry in the i-th row and j-th column of a matrix $A \in M(n,q)$ by A_{ij} [2]. By $H(n)$ we denote the real vector space of Hermitian $n \times n$ matrices. We equip $H(n)$ with the Hilbert-Schmidt inner product and $\|\cdot\|_2$ denotes the Frobenius norm. By $\mathcal{S}^n$ we denote the set of positive semidefinite $n \times n$ matrices and by $\mathcal{S}^n_r \subseteq \mathcal{S}^n$ we denote the subset of positive semidefinite matrices of rank at most r. In the following we assume that $r \in \{1,\dots,\lceil n/2 \rceil - 1\}$ [3]. The set of linear maps $M : H(n) \to \mathbb{R}^m$ is denoted by $\mathcal{M}(m)$.

Definition II.1. *(m-measurement.) An m-measurement is an element of $\mathcal{M}(m)$.*

In the following we denote an m-measurement simply by measurement if we do not want to specify m.

Remark For each m-measurement M there exists a unique $G := (G_1,\dots,G_m) \in H(n)^m$ such that

$$M(X) = \big(\mathrm{tr}(G_1X),\dots,\mathrm{tr}(G_mX)\big)$$

[2] Note that the indices we use to label matrices begin with 0, not with 1.
[3] $\lceil k \rceil :=$ the smallest integer i such that $i \geq k$.

for all $X \in H(n)$. By M_G we denote the m-measurement associated in this way to an $G \in H(n)^m$. In the following we sometimes use this identification to speak of elements $G \in H(n)^m$ as m-measurements.

Definition II.2. *(r-complete.) A measurement M is called r-complete iff $M(X) \neq M(X')$ for all $X \in \mathcal{S}_r^n$ and $X' \in \mathcal{S}^n$ with $X \neq X'$. A tuple $G \in H(n)^m$ is called r-complete iff M_G is r-complete.*

Given a measurement M and a measurement outcome $b = M(X),\ X \in \mathcal{S}_r^n$, consider the following well-known semi-definite program [20, 22, 23] [4]

$$\begin{aligned} &\text{minimize } \operatorname{tr}(Y) \\ &\text{subject to } Y \geq 0,\ M(Y) = b. \end{aligned} \tag{2}$$

The significance of the r-complete property is due to the following observation:

Proposition II.1. *Let M be an r-complete measurement and let $X \in \mathcal{S}_r^n$. If $b = M(X)$, then X is the unique minimizer of the semidefinite program* (2)*.*

Proof. Let $X \in \mathcal{S}_r(\mathbb{C}^n)$ be a Hermitian matrix of rank at most r and let M be an r-complete measurement. Then, X is the unique feasible point of the spectrahedron

$$\{Y \in H(n) : Y \geq 0,\ M(Y) = M(X)\}. \tag{3}$$

This follows immediately from $\{Y \in H(n) : Y \geq 0,\ M(Y) = M(X)\} = \{Y \in \mathcal{S}^n : M(Y) = M(X)\}$ and the definition of r-complete. □

Remark Note that if $\mathbb{1} \in \operatorname{Range}(M^*)$, the r-complete property also is necessary for a deterministic reconstruction via the semidefinite program (2).

This shows that for an r-complete measurement the semidefinite program (2) reduces to a feasibility problem.

Finally, let us state the observation of [19, 25] which gives a useful characterization of the r-complete property:

Proposition II.2. *A measurement M is r-complete if and only if every nonzero $X \in Ker(M)$ has at least $r+1$ positive eigenvalues.*

Proof. Consider the set $\Delta := \{Y - Z : Y \in \mathcal{S}_r^n,\ Z \in \mathcal{S}^n\}$ and note that every $X \in \Delta$ has at most r positive eigenvalues. Furthermore, note that a measurement M is r-complete if and only if $\Delta \cap \operatorname{Ker}(M) \setminus \{0\} = \emptyset$.

Now assume that every $X \in \operatorname{Ker}(M) \setminus \{0\}$ has at least $r+1$ positive eigenvalues. Since every $Y \in \Delta$ has at most r positive eigenvalues we find $Y \notin \operatorname{Ker}(M) \setminus \{0\}$, i.e. $\Delta \cap \operatorname{Ker}(M) \setminus \{0\} = \emptyset$.

Conversely, assume that M is r-complete. Δ clearly contains all matrices with at most r positive eigenvalues and hence $\operatorname{Ker}(M) \setminus \{0\}$ cannot contain an element with r or less positive eigenvalues.

□

[4] This is a convex relaxation of the rank minimization problem.

Remark If every nonzero $X \in \mathrm{Ker}(M)$ has at least $r+1$ positive eigenvalues, then every nonzero $X \in \mathrm{Ker}(M)$ also has at least $r+1$ negative eigenvalues since $X \in \mathrm{Ker}(M)$ implies $-X \in \mathrm{Ker}(M)$.

III. RECONSTRUCTION OF LOW-RANK POSITIVE MATRICES

Our approach relies on [19] where a method to construct the null spaces of r-complete m-measurements for $m = 4r(n-r) + n - 2r$ is provided. Their construction is based on the ideas of [26], details can be found in Appendix A of [19].

First, we focus on the phase retrieval problem.

Theorem III.1. *Let*

$$G := \left(e_0 e_0^*, \ldots, e_{n-1} e_{n-1}^*, \frac{v_1 v_1^*}{\|v_1 v_1^*\|_2}, \frac{\overline{v}_1 \overline{v}_1^*}{\|\overline{v}_1 \overline{v}_1^*\|_2}, \ldots, \frac{v_{2n-3} v_{2n-3}^*}{\|v_{2n-3} v_{2n-3}^*\|_2}, \frac{\overline{v}_{2n-3} \overline{v}_{2n-3}^*}{\|\overline{v}_{2n-3} \overline{v}_{2n-3}^*\|_2} \right),$$

where the v_i are defined in Equation (1)*. If $x_1 < x_2 < \ldots < x_{2n-3}$, then the measurement M_G is* 1*-complete.*

The proof of this theorem can be found in Section V.

Remark From the proof of this result it is easily seen that the kernel of M_G is independent of the choice of the x_i. Thus, for the purpose of robustness, the x_i should be chosen such that the smallest singular value of M_G is maximized.

Let us next state Theorem I.1 in a more precise way.

Corollary III.2. *(Phase Retrieval via PhaseLift.) Let M be a measurement given by Theorem III.1 and let $x \in \mathbb{C}^n$. If $b = M(xx^*)$, then xx^* is the unique minimizer of the semidefinite program* (2)*.*

By Proposition II.1, this is an immediate consequence of Theorem III.1.

Let us next focus on the recovery of low-rank positive matrices. This, however, requires some further definitions: First, let

$$C_r^n := \{X \in H(n) : \mathrm{tr}(X e_i e_j^*) = 0,\ 2r-1 \leq i+j \leq 2(n-r)-1,\ i \neq j,\}. \tag{4}$$

E.g. $C_1^n \subseteq H(n)$ is the subspace of $n \times n$ diagonal matrices and C_3^7 is the subspace of $H(7)$ of the from

$$\begin{pmatrix} * & * & * & * & * & 0 & 0 \\ * & * & * & * & 0 & 0 & 0 \\ * & * & * & 0 & 0 & 0 & * \\ * & * & 0 & * & 0 & * & * \\ * & 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & * & * & * & * & * \end{pmatrix}.$$

For $x \in \mathbb{R}\setminus\{0\}$, $k \in \{2r-1,\dots,2(n-r)-1\}$, define the Hermitian matrices $R_k(x), I_k(x) \in (C_r^n)^\perp$ by [5]

$$(R_k(x))_{jl} := \delta_{j+l,k} x^j,\ j,l \in \{0,\dots,n-1\},\ j>l,$$
$$(I_k(x))_{jl} := i\delta_{j+l,k} x^j,\ j,l \in \{0,\dots,n-1\},\ j>l,$$

where $\delta_{i,j}$ denotes the Kronecker delta. E.g. for $n=5$, $r=2$ these are

$$R_3(x) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & x & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, I_3(x) = \begin{pmatrix} 0 & 0 & 0 & i & 0 \\ 0 & 0 & ix & 0 & 0 \\ 0 & -ix & 0 & 0 & 0 \\ -i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, R_4(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, I_4(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & i \\ 0 & 0 & 0 & ix & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -ix & 0 & 0 & 0 \\ -i & 0 & 0 & 0 & 0 \end{pmatrix},$$
$$R_5(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}, I_5(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & i \\ 0 & 0 & 0 & ix & 0 \\ 0 & 0 & -ix & 0 & 0 \\ 0 & -i & 0 & 0 & 0 \end{pmatrix}.$$

Theorem III.3. *Let G_0 be a basis of C_r^n and let $x_1, x_2, \dots, x_r \in \mathbb{R}\setminus\{0\}$ with $x_1 < x_2 < \dots < x_r$. For $k \in \{2r-1,\dots,2(n-r)-1\}$ define*

$$G_k := (I_k(x_1), R_k(x_1), \dots, I_k(x_r), R_k(x_r)).$$

and let $G := G_0 \cup G_{2r-1} \cup \dots \cup G_{2(n-r)-1}$ [6]. Then the measurement M_G is r-complete and $|G| = 4r(n-r)+n-2r$.

Remark If an m-measurement is injective when restricted to $\mathcal{S}_r^n$, it was shown in [6, 27] that, up to terms at most logarithmic in n, we have $m \geq 4r(n-r)$. Furthermore, in [3, 6] it was shown that there indeed exist injective m-measurements for $m = 4r(n-r)$. Thus, it might be worth noting that the measurements given by Theorem III.3 solely require $n-2r$ additional measurement outcomes as compared to the nearly optimal bound $4r(n-r)$.

Finally, by Proposition II.1, the measurements given by Theorem III.3 allow for the recovery of low-rank positive matrices.

Corollary III.4. *(Recovery of low-rank positive matrices.) Let M be a measurement given by Theorem III.3 and let $X \in \mathcal{S}_r^n$. If $b = M(X)$, then X is the unique minimizer of the semidefinite program* (2).

IV. STABILITY

In this section we discuss the stability of r-complete measurements.

Assume there is an error term $E \in H(n)$ that perturbs the matrix $X_r \in \mathcal{S}_r^n$ we intend to recover to the matrix $X = X_r + E$. Measuring with an r-complete measurement M yields

[5] As $R_k(x), I_k(x) \in (C_r^n)^\perp$ both have vanishing diagonal and since they are hermitian, it suffices to define all elements above the diagonal.

[6] For tuples of Hermitian matrices $X := (X_1,\dots,X_i) \in H(n)^i$, $Y := (Y_1,\dots,Y_j) \in H(n)^j$ we define their union $X \cup Y$ to be the tuple $X \cup Y := (X_1,\dots,X_i,Y_1,\dots,Y_j) \in H(n)^{i+j}$.

the perturbed outcome $b = M(X)$. Clearly, the matrix X_r cannot always be perfectly recovered from the outcome b, however, if $\|M(E)\|_2$ is small, there is a recovery procedure that yields a matrix close to X_r. For that purpose, consider the following well-known optimization problem

$$\begin{aligned} &\text{minimize } \operatorname{tr}(Y) \\ &\text{subject to } Y \geq 0,\ \|M(Y) - b\|_2 \leq \epsilon \end{aligned} \tag{5}$$

where $\epsilon \geq 0$ is a constant representing the error scale.

Theorem IV.1. *(Stable recovery of low-rank positive matrices.) Let M be an r-complete measurement and let $\epsilon > 0$. There is a constant $C_M > 0$ independent of ϵ such that for all $X_r \in \mathcal{S}_r^n$ and $E \in H(n)$ with $\|M(E)\|_2 \leq \epsilon$, any minimizer Y of (5) for $b = M(X_r + E)$ satisfies*

$$\|Y - X_r\|_2 \leq C_M \epsilon.$$

Remark In the proof of this theorem we show that $C_M \leq \frac{2}{\sigma_{\min}}(1 + \frac{1}{\kappa})$ where σ_{min} is the smallest singular value of M and $\kappa := -\max_{Z \in \operatorname{Ker}(M), \|Z\|_2 = 1} \lambda_{n-r}(Z)$ [7]. However we do not know how to compute κ for a given r-complete measurement M and hence we cannot make this bound more explicit.

The proof of this theorem can be found in Section V. In order for this result to be a practical stability guarantee, one would have to estimate the constant C_M. At this point we do not know how this can be achieved. In order to indicate the magnitude of the constant C_M, let us next present some numerical results. For this purpose consider the tuple

$$G_n := \left(e_0 e_0^*, \ldots, e_{n-1} e_{n-1}^*, \frac{I_1(1)}{\|I_1(1)\|_2}, \frac{R_1(1)}{\|R_1(1)\|_2}, \ldots, \frac{I_{2n-3}(1)}{\|I_{2n-3}(1)\|_2}, \frac{R_{2n-3}(1)}{\|R_{2n-3}(1)\|_2} \right)$$

and note that by Theorem III.3 the associated measurement M_{G_n} is 1-complete. Figure 1 presents numerical results that might indicate the scaling of $C_{M_{G_n}}$ for the sequence of measurements $(M_{G_n})_{n \in \mathbb{N}}$.

Just like in [12], this recovery scheme can also be used for the phase retrieval problem. For a Hermitian matrix $A \in H(n)$, we denote by $\operatorname{Eig}(A) \in \mathbb{R}^n$ the tuple of eigenvalues of A ordered decreasingly together with their multiplicities. Furthermore, we define $\lambda_i(A) := \operatorname{Eig}(A)_{i-1},\ i \in \{1, \ldots, n\}$.

Proposition IV.2. *(Stability for Phase Retrieval.) Let $X = xx^* + E$, where $x \in \mathbb{C}^n$ is the signal and $E \in H(n)$ is an error term. Let M be a 1-complete measurement and let $\epsilon \geq \|M(E)\|_2$. Furthermore, let Y be any minimizer of the optimization problem (5) for $b = M(X)$ and set $\hat{x} := \sqrt{\lambda_1(Y)} x'$ where $x' \in S^{n-1}$ is an eigenvector of Y with eigenvalue $\lambda_1(Y)$. Then*

$$\|xx^* - \hat{x}\hat{x}^*\|_2 \leq 2 C_M \epsilon,$$

[7] λ_{n-r} is defined later this section.

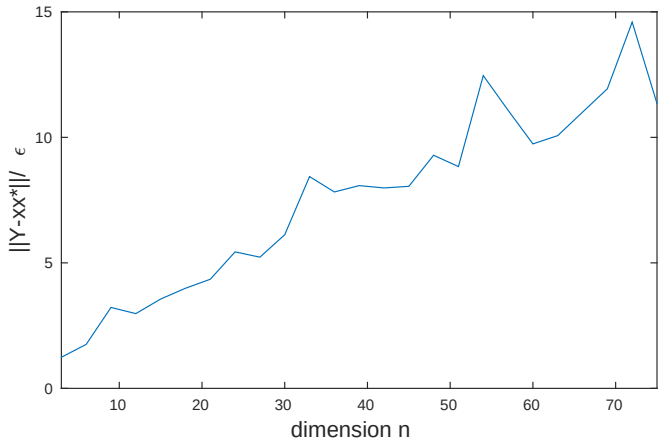

FIG. 1: For each $n \in \{3, 6, \ldots, 75\}$ we choose uniformly at random a normalized vector $x \in \mathbb{C}^n$ and an error term $f \in \mathbb{R}^{5n-6}$ with $\|f\|_2 \leq \epsilon := 10^{-3}$. Then we run the program (5) with the outcome $b = M_{G_n}(xx^*) + f$. The figure shows the maximum value of $\|Y - xx^*\|_2/\epsilon$ for 2200 repetitions where Y is the minimizer of (5).

where C_M is the constant given by Theorem IV.1. Furthermore, for some $\varphi \in [0, 2\pi)$ we have

$$\|x - e^{i\varphi}\hat{x}\|_2 \leq \frac{2\sqrt{2}C_M}{\|x\|_2}\epsilon.$$

This result follows from Theorem IV.1 by a straightforward computation. The proof is given in Section V.

Remark The proofs of V.5 shows that the above stability results also hold true the following recovery scheme:

$$\begin{aligned} &\text{minimize } \|M(Y) - b\|_2 \\ &\text{subject to } Y \geq 0, \end{aligned} \tag{6}$$

where M is r-complete and $b = M(X_r + E)$, $X_r \in \mathcal{S}_r^n$.

V. TECHNICAL APPENDIX

Let us first introduce some notation we use throughout this section. Let $A \in M(n, q)$, $i \in \{0, \ldots, n-1\}$, $j \in \{0, \ldots, q-1\}$. By $A_{,i}$ we denote the $(n-1) \times q$ matrix obtained from A by deleting the i-th row and by $A^{,j}$ we denote the $n \times (q-1)$ matrix obtained from A by deleting the j-th column. By $A\{i\}$ we denote the i-th row of A and by $A[j]$ we denote the j-th column of A. Furthermore, for $k \in \{0, \ldots, n+q-2\}$, we denote the k-th anti-diagonal of A by $A(k)$, i.e. $A(k) := (A_{ij})_{i+j=k}$ [8].

[8] The ordering is such that the matrix element with smaller i comes first.

A. Proof of Theorem III.3

Since Theorem III.1 is obtained by manipulating the measurements obtained from Theorem III.3 we begin by proving the latter. The construction we give in the following yields a more general class of r-complete measurements than the ones given by Theorem III.3 and it strongly relies on the notion of totally non-singular matrices.

Definition V.1. *(Totally non-singular.) A matrix $A \in M(n,q)$ is called totally non-singular if A has no vanishing minor.*

The following lemma is a central ingredient for the construction given in the following.

Lemma V.1. *Let $q \in \{1,\dots,n-1\}$ and let $A \in M(n,q)$ be totally non-singular. Then, there exists a totally non-singular matrix $B \in M(n,n-q)$ such that $A^*B = 0$.*

Proof. We give a proof by induction in the dimension n for q fixed.

Base case. Let us begin with the base case $n = q+1$. Note that for a given $A \in M(q+1,q)$ there always exists a nonzero matrix (actually just a vector) $B \in M(q+1,1)$ such that $A^*B = 0$, in particular if A is totally non-singular.

Since B exists, it is enough to prove that if A is totally non-singular B is totally non-singular as well: Assume for a contradiction that B is not totally non-singular, i.e. that B has a vanishing entry. By permuting rows we can assume A and B to be of the form

$$A = \begin{pmatrix} F \\ D \end{pmatrix}, \quad B = \begin{pmatrix} 0 \\ E \end{pmatrix}$$

for some matrices $F \in M(1,q)$, $D \in M(q,q)$ and $E \in M(q,1)$. But then

$$A^*B = F^*0 + D^*E = D^*E = 0.$$

In particular this implies that the $q \times q$ submatrix D of A is singular, contradicting the fact that A is totally non-singular by assumption.

Induction step. Assume the claim holds for an $n > q$ and let $A \in M(n+1,q)$ be totally non-singular. Note that for each $i \in \{0,\dots,n\}$, the $n \times q$ matrix $A_{,i}$ is totally non-singular since A is totally non-singular. Thus, by the induction hypothesis, we can find for each $i \in \{0,\dots,n\}$ a totally non-singular matrix $C_i \in M(n,n-q)$ such that $A^*_{,i}C_i = 0$. For $i \in \{0,\dots,n\}, j \in \{0,\dots,n-q\}$ let $C(i,j) \in M(n+1,n+1-q)$ be the matrix with $C(i,j)^{,j}_{,i} = C_i$ and 0 else. Then, for all $i \in \{0,\dots,n\}, j \in \{0,\dots,n-q\}$, $C(i,j)^{,j}_{,i}$ is totally non-singular, $C(i,j)[j] = 0$ and $A^*C(i,j) = 0$ by construction.

Step 1. First, for each $i \in \{0,\dots,n\}$, we deform $C(i,0)$ into a matrix $\tilde{C}(i,0) \in M(n+1,n+1-q)$ with the following properties:

1. $A^*\tilde{C}(i,0) = 0$,
2. $\tilde{C}(i,0)^{,0}_{,i}$ is totally non-singular,
3. All $(n+1-q)\times(n+1-q)$ minors of $\tilde{C}(i,0)_{,i}$ are nonzero.

Let $i \in \{0,\dots,n\}$. For $\sigma := (k_0,\dots,k_{n-q}) \in \Sigma := \{(l_0,\dots,l_{n-q}) : 0 \le l_0 < \dots < l_{n-q} \le n-1\}$ define the projection $P_\sigma : M(n+1,n+1-q) \to M(n+1-q,n+1-q)$ by $P_\sigma(X)\{j\} := (X_{,i})\{k_j\}$ for all $X \in M(n+1,n+1-q), j \in \{0,\dots,n-q\}$. Now let $\sigma \in \Sigma$, and set $E_\sigma := P_\sigma(C(i,0))$. By permuting rows we can assume A and $C(i,0)$ to be of the form

$$A = \begin{pmatrix} F \\ D \end{pmatrix}, \quad C(i,0) = \begin{pmatrix} E_\sigma \\ F_\sigma \end{pmatrix} \tag{7}$$

for some matrices $F \in M(n+1-q,q)$, $D \in M(q,q)$ and $F_\sigma \in M(q,n+1-q)$.

Next, we show that there is a vector $u_\sigma = \begin{pmatrix} v_\sigma \\ w_\sigma \end{pmatrix}$ [9], where $v_\sigma \in \mathbb{C}^{n+1-q}$, $w_\sigma \in \mathbb{C}^q$, such that $A^* u_\sigma = 0$ and $\det(E_\sigma + P_\sigma(u_\sigma e_0^*)) = \det(E_\sigma + v_\sigma e_0^*) \neq 0$: Since C_i is totally non-singular, E_σ has rank $n-q$. Thus we can find a vector $v_\sigma \in \mathbb{C}^{n+1-q}$ such that $\det(E_\sigma + v_\sigma e_0^*) \neq 0$ [10]. Finally, we just have to ensure that $A^* u_\sigma = 0$. Since D is totally non-singular there is a vector $w_\sigma \in \mathbb{C}^q$ such that $D^* w_\sigma = -F^* v_\sigma$ and this gives $A^* \begin{pmatrix} v_\sigma \\ w_\sigma \end{pmatrix} = F^* v_\sigma + D^* w_\sigma = 0$. Repeating this construction, we can find a collection of vectors $\{u_\sigma\}_{\sigma\in\Sigma} \subseteq \mathbb{C}^{n+1}$ such that for all $\sigma \in \Sigma$ we have $A^* u_\sigma = 0$ and $\det\big(P_\sigma(C(i,0) + u_\sigma e_0^*)\big) \neq 0$.

Next, for distinct $\sigma_1, \sigma_2 \in \Sigma$, define the mapping $K(\lambda) := C(i,0) + u_{\sigma_1} e_0^* + \lambda u_{\sigma_2} e_0^*$, $\lambda \in \mathbb{C}$ and note that by construction $A^* K(\lambda) = 0$ for all $\lambda \in \mathbb{C}$. Note that by construction $K(\lambda)_{,i}^{,0} = C_i$ is totally non-singular for all λ. Furthermore, the $(n+1-q) \times (n+1-q)$ minors $\det\big(P_{\sigma_1}(K(\lambda))\big)$ and $\det\big(P_{\sigma_2}(K(\lambda))\big)$ can be considered as polynomials in λ. The polynomial equations $\det\big(P_{\sigma_1}(K(\lambda))\big) = 0$ and $\det\big(P_{\sigma_2}(K(\lambda))\big) = 0$ are non-trivial: For $\lambda = 0$ we have $\det\big(P_{\sigma_1}(K(0))\big) = \det\big(P_{\sigma_1}(C(i,0) + u_{\sigma_1} e_0^*)\big) \neq 0$ by construction. For λ large one can consider $\frac{1}{\lambda} u_{\sigma_1} e_0^*$ as a small perturbation to $u_{\sigma_2} e_0^*$. Thus, using linearity of the determinant in the 0-th column, we conclude that

$$\begin{aligned} \det\big(P_{\sigma_2}(K(\lambda))\big) &= \det\big(P_{\sigma_2}(C(i,0) + u_{\sigma_1} e_0^* + \lambda u_{\sigma_2} e_0^*)\big) \\ &= \lambda \cdot \det\big(P_{\sigma_2}(C(i,0) + u_{\sigma_2} e_0^*) + \frac{1}{\lambda} P_{\sigma_2}(u_{\sigma_1} e_0^*)\big) \neq 0 \end{aligned}$$

for large enough λ by the continuity of the determinant and the fact that $\det\big(P_{\sigma_2}(C(i,0) + u_{\sigma_2} e_0^*)\big) \neq 0$ by construction. A non-trivial polynomial equation in one variable just has a finite set of solutions and hence the set

$$\begin{aligned} &\{\lambda \in \mathbb{C} : \det\big(P_{\sigma_1}(K(\lambda))\big) = 0 \vee \det\big(P_{\sigma_2}(K(\lambda))\big) = 0\} \\ = &\{\lambda \in \mathbb{C} : \det\big(P_{\sigma_1}(K(\lambda))\big) = 0\} \cup \{\lambda \in \mathbb{C} : \det\big(P_{\sigma_2}(K(\lambda))\big) = 0\} \end{aligned}$$

is finite. In particular there is an $a_{\sigma_2} \in \mathbb{C}$ such that $\det\big(P_{\sigma_1}(K(a_{\sigma_2}))\big) \neq 0$ and $\det\big(P_{\sigma_2}(K(a_{\sigma_2}))\big) \neq 0$ [11]. Applying the same argument to $L(\lambda) := C(i,0) + u_{\sigma_1} e_0^* +$

[9] The direct sum decomposition of u_σ is with respect to the decomosition given by Equation (7), i.e. $A^* u_\sigma = F^* v_\sigma + D^* w_\sigma$.

[10] Note that $E_\sigma[0] = 0$ by construction of $C(i,0)$.

[11] In fact this holds for almost all $a_{\sigma_2} \in \mathbb{C}$.

$a_{\sigma_2}u_{\sigma_2}e_0^* + \lambda u_{\sigma_3}e_0^*$, $\lambda \in \mathbb{C}$, where $\sigma_3 \in \Sigma$ is distinct from σ_1, σ_2, yields an $a_{\sigma_3} \in \mathbb{C}$ such that $\det\big(P_{\sigma_1}(L(a_{\sigma_3}))\big) \neq 0$, $\det\big(P_{\sigma_2}(L(a_{\sigma_3}))\big) \neq 0$ and $\det\big(P_{\sigma_3}(L(a_{\sigma_3}))\big) \neq 0$ [12]. Finally, since $|\Sigma|$ is finite, we can inductively apply the argument to obtain a matrix $\tilde{C}(i,0) = C(i,0) + u_{\sigma_1}e_0^* + \sum_{\sigma\in\Sigma,\sigma\neq\sigma_1} a_\sigma u_\sigma e_0^*$ with the desired properties.

Step 2. Secondly, we construct for each $i \in \{0,\dots,n\}$ a matrix $D_i \in M(n+1,q)$ with the following properties:

1. $A^*D_i = 0$.

2. $(D_i)_{,i}$ is totally non-singular.

Let $i \in \{0,\dots,n\}$. Let $D_i(\lambda_1,\dots,\lambda_{n-q}) := \tilde{C}(i,0) + \sum_{j=1}^{n-q}\lambda_j C(i,j)$ where $\lambda_j \in \mathbb{C}$, $j \in \{1,\dots,n-q\}$, and note that by construction we have $A^*D_i(\lambda_1,\dots,\lambda_{n-q}) = 0$ for all $\lambda_1,\dots,\lambda_{n-q} \in \mathbb{C}$. By choosing $(\lambda_1,\dots,\lambda_{n-q})$ appropriately one can make sure that $(D_i(\lambda_1,\dots,\lambda_{n-q}))_{,i}$ is totally non-singular: First let $G(\lambda) := \tilde{C}(i,0) + \lambda C(i,1)$, $\lambda \in \mathbb{C}$. Just like in Step 1, the minors of $G(\lambda)^{,0}_{,i}$ and $G(\lambda)^{,1}_{,i}$ together with the $(n+1-q)\times(n+1-q)$ minors of $G(\lambda)_{,i}$ yield a finite set of polynomial equations in λ. All of these polynomial equations are non-trivial: For $\lambda = 0$ none of the minors of $G(0)^{,0}_{,i} = C_i$ and none of the $(n+1-q)\times(n+1-q)$ minors of $G(0)_{,i} = \tilde{C}(i,0)_{,i}$ vanish by construction of $\tilde{C}(i,0)$. For large λ one can consider $\frac{1}{\lambda}\tilde{C}(i,0)$ as a small perturbation to $C(i,1)$. Hence, for large enough λ, none of the minors of $\frac{1}{\lambda}G(\lambda)^{,1}_{,i}$ vanishes by the fact that $C(i,1)^{,1}_{,i} = C_i$ is totally non-singular by construction and the continuity of the minors. Thus, just like in Step 1, we conclude that there are just finitely many values of λ for which any of these polynomials vanishes. In particular there is an $\lambda_1 \in \mathbb{C}$ such that both $G(\lambda_1)^{,0}_{,i}$ and $G(\lambda_1)^{,1}_{,i}$ are totally non-singular and all $(n+1-q)\times(n+1-q)$ minors of $G(\lambda_1)_{,i}$ are nonzero. Applying the same argument to $H(\lambda) := \tilde{C}(i,0) + \lambda_1 C(i,1) + \lambda C(i,2)$, $\lambda \in \mathbb{C}$, yields an $\lambda_2 \in \mathbb{C}$ such that $H(\lambda_2)^{,0}_{,i}$, $H(\lambda_2)^{,1}_{,i}$ and $H(\lambda_2)^{,2}_{,i}$ are totally non-singular and all $(n+1-q)\times(n+1-q)$ minors of $H(\lambda_2)_{,i}$ are nonzero. Choosing the values for λ_j, $j \in \{1,\dots,n-q\}$, inductively in this fashion finally yields a matrix D_i with the desired properties.

Step 3. To complete the induction step we choose by a similar argument as in Step 1 and Step 2 before parameters $\gamma_j \in \mathbb{C}$, $j \in \{1,\dots,n\}$, in $B := D_0 + \sum_{j=1}^{n}\gamma_j D_j$ such that $B_{,i}$ is totally non-singular for each $i \in \{0,\dots,n\}$, i.e. such that B is totally non-singular: First define $I(\lambda) := D_0 + \lambda D_1$, $\lambda \in \mathbb{C}$. Clearly $I(0)_{,0} = (D_0)_{,0}$ is totally non-singular by construction of D_0. Furthermore, for large λ , $\frac{1}{\lambda}D_0$ can be considered as a small perturbation to D_1. Thus, for λ large enough, $\frac{1}{\lambda}I(\lambda)_{,1}$ is totally non-singular by construction of D_1 and the continuity of the minors. Hence, all the minors of $I(\lambda)_{,0}$ and $I(\lambda)_{,1}$ yield non-trivial polynomial equations in λ and therefore there are just finitely many values for λ for which any of these minors vanishes. In particular there is a $\gamma_1 \in \mathbb{C}$ such that both $I(\gamma_1)_{,0}$ and $I(\gamma_1)_{,1}$ are totally non-singular. Applying the same argument to $J(\lambda) := D_0 + \gamma_1 D_2 + \lambda D_2$ yields a $\gamma_2 \in \mathbb{C}$ such that $J(\gamma_2)_{,0}$, $J(\gamma_2)_{,1}$ and $J(\gamma_2)_{,2}$ are totally non-singular. Continuing to choose the γ_i, $i \in \{1,\dots,n\}$, inductively in this fashion then yields a totally non-singular matrix B with $A^*B = 0$. □

[12] Also in this case we obtain a finite set of non-trivial polynomial equations in λ and thus the argument given before can be applied to find a_{σ_3}.

Lemma V.2. *Let $q \in \{1, \dots, n-1\}$ and let $A \in M(n, q, \mathbb{R})$ be totally non-singular. Then, there exists a totally non-singular matrix $B \in M(n, n-q, \mathbb{R})$ such that $A^t B = 0$.*

Proof. The arguments given in the proof of Lemma V.1 also apply to real numbers. □

For $k \in \{1, \dots, 2n-3\}$, define the inclusion in the k-th antidiagonal $\iota_k : \mathbb{C}^{\gamma(n,k)} \to H(n)$ by

$$(\iota_k(v))_{jl} := \frac{1}{\sqrt{2}} \begin{cases} v_j & \text{if } j+l=k, j<l \\ v_l^* & \text{if } j+l=k, l<j \\ 0 & \text{else} \end{cases}$$

where

$$\gamma(n,k) = \begin{cases} \lceil k/2 \rceil & \text{if } k \leq n-1 \\ \lceil n-1-k/2 \rceil & \text{if } k > n-1 \end{cases}$$

is the length of the upper half of the k-th antidiagonal. By expanding in the generalised Gell-Mann orthonormal basis of $H(n)$, it is easily seen that the inclusion of real vectors in the same antidiagonal preserves the standard inner product, i.e. for $k \in \{1, \dots, 2n-3\}$ we have

$$\operatorname{tr}\big(\iota_k(v)\iota_k(w)\big) = \langle v, w \rangle, \ \forall v, w \in \mathbb{R}^{\gamma(n,k)}. \tag{8}$$

Furthermore, the inclusion of an imaginary and a real vector in the same antidiagonal yields Hilbert-Schmidt orthogonal matrices, i.e. for $k \in \{1, \dots, 2n-3\}$ we have

$$\operatorname{tr}\big(\iota_k(v)\iota_k(iw)\big) = 0, \ \forall v, w \in \mathbb{R}^{\gamma(n,k)}, \tag{9}$$

and finally that inclusions of vectors in different antidiagonals also yield Hilbert-Schmidt orthogonal matrices, i.e. for $k, j \in \{1, \dots, 2n-3\}$ with $k \neq j$ we have

$$\operatorname{tr}\big(\iota_k(v)\iota_j(w)\big) = 0, \ \forall v \in \mathbb{C}^{\gamma(n,k)}, w \in \mathbb{C}^{\gamma(n,j)}. \tag{10}$$

The following theorem is the main result of the present paper.

Theorem V.3. *Let G_0 be a basis of C_r^n* [13]*. Furthermore, for $k \in \{2r-1, \dots, 2(n-r)-1\}$, let $A_k, A'_k \in M(\gamma(n,k), r, \mathbb{R})$ be totally non-singular and define the tuple*

$$G_k := \big(\iota_k(A_k[0]), \iota_k(iA'_k[0]), \iota_k(A_k[1]), \iota_k(iA'_k[1]), \dots, \iota_k(A_k[r-1]), \iota_k(iA'_k[r-1])\big).$$

Then $G := G_0 \cup G_{2r-1} \cup G_{2r} \cup \cdots \cup G_{2(n-r)-1}$ is r-complete and $|G| = 4r(n-r) + n - 2r$.

[13] C_r^n was defined in Equation (4).

Proof. The idea of the proof is to use Lemma V.2 to determine a basis of the null space of M_G such that the construction of [19] can be applied. We do this in the first step of the proof. In the second step of the proof we use the construction of [19] to show that M_G indeed is r-complete.

Step 1. First, by Lemma V.2, there are totally non-singular $B_k, B'_k \in M(\gamma(n,k), \gamma(n,k)-r, \mathbb{R})$, $k \in \{2r+1, \dots, 2(n-r)-3\}$, such that

$$\begin{aligned} A_k^t B_k &= 0, \\ (A'_k)^t B'_k &= 0. \end{aligned} \tag{11}$$

Now let

$$G_k^\perp := \big(\iota_k(B_k[0]), \iota_k(iB'_k[0]), \dots, \iota_k(B_k[\gamma(n,k)-r-1]), \iota_k(iB'_k[\gamma(n,k)-r-1])\big), \quad k \in \{2r+1, \dots, 2(n-r)-3\}$$

and let $G_k^\perp = (0)$ for $k \in \{2r-1, 2r, 2(n-r)-2, 2(n-r)-1\}$. In the remainder of this first step we prove that $G_{2r-1}^\perp \cup \dots \cup G_{2(n-r)-1}^\perp$ is a basis of $\mathrm{Ker}(M_G)$: For $k \in \{1, \dots, 2n-3\}$, let $Q_k := \{X \in H(n) : X(j) = 0 \ \forall j \neq k \ \wedge \ X_{ii} = 0 \text{ for } 2i = k\}$ be the subspace of Hermitian matrices with vanishing diagonal and non-vanishing entries only in the k-th antidiagonal. By Equation (10), $H(n)$ can be decomposed into the following mutually orthogonal subspaces:

$$H(n) = C_r^n \oplus Q_{2r-1} \oplus \dots \oplus Q_{2(n-r)-1}. \tag{12}$$

Note that $\mathrm{Span}(G_k \cup G_k^\perp) \subseteq Q_k$ for all $k \in \{2r-1, \dots, 2(n-r)-1\}$. Hence, by the decomposition (12), to show that $G_{2r-1}^\perp \cup \dots \cup G_{2(n-r)-1}^\perp$ is a basis of $\mathrm{Ker}(M_G)$ it suffices to prove that for $k \in \{2r-1, \dots, 2(n-r)-1\}$ the matrices $G_k^\perp \cup G_k$ span the subspace Q_k and that $\mathrm{Span}(G_k^\perp) \subseteq \mathrm{Ker}(M_G)$. First observe that indeed $\mathrm{Span}(G_k^\perp) \subseteq \mathrm{Ker}(M_G)$ for every $k \in \{2r+1, \dots, 2(n-r)-3\}$: Note that for every $k \in \{2r+1, \dots, 2(n-r)-3\}$,

$$\begin{aligned} \mathrm{tr}\big(\iota_k(A_k[l])\iota_k(B_k[j])\big) &= \langle A_k[l], B_k[j]\rangle = (A_k^t B_k)_{lj} = 0, \\ \mathrm{tr}\big(\iota_k(iA'_k[l])\iota_k(iB'_k[j])\big) &= \langle A'_k[l], B'_k[j]\rangle = ((A'_k)^t B'_k)_{lj} = 0, \\ \forall l \in \{0, \dots, r-1\},\ j &\in \{0, \dots, \gamma(n,k)-r-1\}, \end{aligned} \tag{13}$$

by equations (8) and (11). Furthermore,

$$\begin{aligned} \mathrm{tr}\big(\iota_k(iA'_k[l])\iota_k(B_k[j])\big) &= 0, \\ \mathrm{tr}\big(\iota_k(A_k[l])\iota_k(iB'_k[j])\big) &= 0, \\ \forall l \in \{0, \dots, r-1\},\ j &\in \{0, \dots, \gamma(n,k)-r-1\}, \end{aligned} \tag{14}$$

by Equation (9). I.e. $\mathrm{Span}(G_k^\perp)$ is orthogonal to $\mathrm{Span}(G_k)$ and thus $\mathrm{Span}(G_k^\perp) \subseteq \mathrm{Ker}(M_G)$.

To conclude the first step, we prove that $G_k^\perp \cup G_k$ spans the subspace Q_k for every $k \in \{2r-1, \dots, 2(n-r)-1\}$: Let $k \in \{2r-1, \dots, 2(n-r)-1\}$. Since A_k is totally non-singular, the columns of A_k are linearly independent and the same argument applies to A'_k. Hence, by the equations (8) and (9), G_k is a tuple of linearly independent Hermitian

matrices. The same argument applies to $G_k^\perp$, $k \in \{2r+1, \ldots, 2(n-r)-3\}$. But we have seen that $\mathrm{Span}(G_k)$ is orthogonal to $\mathrm{Span}(G_k^\perp)$ for $k \in \{2r+1, \ldots, 2(n-r)-3\}$. Furthermore, for $k \in \{2r-1, \ldots, 2(n-r)-1\}$, $|G_k^\perp| + |G_k| = 2(\gamma(n,k) - r) + 2r = 2\gamma(n,k) = \dim Q_k$ and thus $G_k^\perp \cup G_k$ indeed spans Q_k.

Finally, observe that

$$\begin{aligned} |G| &= \dim C_r^n + \sum_{i=2r-1}^{2(n-r)-1} |G_i| = \sum_{i=1}^{2r-2} 2\gamma(n,i) + n + \sum_{i=1}^{2(n-2r)+1} 2r \\ &= (2r)^2 - 2(2r) + n + 2r(2(n-2r)+1) \\ &= 4r(n-r) + n - 2r. \end{aligned}$$

Step 2. In the second step, we essentially reproduce the construction of [19] and some ideas of [26]. We show in the following that every nonzero matrix $X \in \mathrm{Ker}(M_G)$ has at least $r+1$ positive and $r+1$ negative eigenvalues and this concludes the proof by Proposition II.2.

Let $X \in \mathrm{Ker}(M_G)$ be arbitrary. By the interlaced eigenvalue Theorem (Theorem 4.3.15 of [28]) it suffices to prove that there is an $2(r+1) \times 2(r+1)$ principal submatrix of X with $r+1$ positive and $r+1$ negative eigenvalues. We conclude the proof by finding such a submatrix: There is a smallest number $k \in \{2r+1, \ldots, 2(n-r)-3\}$ such that X has non-vanishing entries in the k-th antidiagonal. First note that either the real or the imaginary part of the k-th antidiagonal does not vanish. Let us consider the case where the real part does not vanish, the other case can be shown analogously. The real part of the k-th antidiagonal of $\mathrm{Ker}(M_G)$ is spanned by the $\gamma(n,k) - r$ real matrices of $G_k^\perp$, i.e. each $X \in \mathrm{Ker}(M_G)$ is a linear combination of the $\gamma(n,k) - r$ real matrices of $G_k^\perp$. But then there have to be at least $2(r+1)$ non-vanishing entries in the k-th antidiagonal of X because otherwise there would be a vanishing $(\gamma(n,k)-r) \times (\gamma(n,k)-r)$ minor of B_k and this contradicts the fact that B_k is totally non-singular (For more details see Lemma 9 of [26].). I.e. there is a $2(r+1) \times 2(r+1)$ principal submatrix of X of the from:

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & \overline{x}_1 \\ 0 & 0 & 0 & \ldots & 0 & \overline{x}_2 & \overline{y}_1^1 \\ 0 & 0 & 0 & \ldots & \overline{x}_3 & \overline{y}_1^2 & \overline{y}_2^1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & x_3 & \ldots & 0 & \overline{y}_{2r-2}^2 & \overline{y}_{2r-1}^1 \\ 0 & x_2 & y_1^2 & \ldots & y_{2r-2}^2 & 0 & \overline{y}_{2r}^1 \\ x_1 & y_1^1 & y_2^1 & \ldots & y_{2r-1}^1 & y_{2r}^1 & 0 \end{pmatrix}, x_i \in \mathbb{C} \setminus \{0\},\ i \in \{1, \ldots, r+1\}, \tag{15}$$

where $y_i^j \in \mathbb{C},\ j \in \{1, \ldots, r\}, i \in \{1, \ldots, 2(r+1) - 2j\}$, are arbitrary.

Finally, we show by induction that a matrix of this form has at least $r+1$ positive and $r+1$ negative eigenvalues: The claim clearly holds for $r = 0$. Now assume the claim holds for $r \in \mathbb{N}_0$. Let Y be a $2(r+2) \times 2(r+2)$ matrix that is of the form illustrated in Equation (15). Then, one can obtain a principal $2(r+1) \times 2(r+1)$ submatrix Y' of Y that is of the same form by e.g. deleting the first and last row as well as the first and last column of Y. Thus, by the induction hypothesis and the interlaced eigenvalue Theorem

(Theorem 4.3.15 of [28]), Y has at least $r+1$ positive and $r+1$ negative eigenvalues. A straightforward calculation shows that $\det(Y)\cdot\det(Y')<0$. Since the determinant of a matrix is the product of its eigenvalues, the claim follows from $\det(Y)\cdot\det(Y')<0$. □

In the following the $r=1$ case is of particular interest because Theorem III.1 is obtained from this case by choosing the totally non-singular matrices appropriately.

Corollary V.4. *Let $G_0 := (e_0 e_0^*, \ldots, e_{n-1}e_{n-1}^*)$. Furthermore let $w_k, v_k \in \mathbb{R}^{\gamma(n,k)}$, $k \in \{1,\ldots,2n-3\}$, be such that every entry of v_k and every entry of w_k is nonzero. Then $G := G_0 \cup \big(\iota_1(v_1), \iota_1(iw_1)\big) \cup \cdots \cup \big(\iota_{2n-3}(v_{2n-3}), \iota_{2n-3}(iw_{2n-3})\big)$ is 1-complete and $|G| = 5n-6$.*

Proof. First, note that G_0 is a basis of C_1^n. Furthermore as by assumption all entries of matrices $w_k, v_k \in \mathbb{R}^{\gamma(n,k)} \simeq M(\gamma(n,k),1,\mathbb{R})$, $k \in \{1,\ldots,2n-3\}$, are nonzero, we conclude that all their minors are nonzero[14]. Consequently the matrices $w_k, v_k \in M(\gamma(n,k),1,\mathbb{R})$, $k \in \{1,\ldots,2n-3\}$, are totally non-singular. Hence G_0 and $G_k := \big(\iota_1(v_1), \iota_1(iw_1)\big)$, $k \in \{1,\ldots,2n-3\}$ fulfil the conditions of Theorem V.3 for $r=1$ and thus $G = G_0 \cup G_1 \cup \ldots \cup G_{2n-3}$ is 1-complete. □

Example For $i \in \{1,\ldots,2n-3\}$, we can choose $w_i = v_i = \sqrt{2}e$, where $e := (1,\ldots,1) \in \mathbb{R}^{\gamma(n,i)}$ is the vector with a one in every component. Altogether this yields $2(2n-3)+n = 5n-6$ Hermitian operators for G. For $n=4$ these are

$$\begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{pmatrix}, \begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}, \begin{pmatrix}0&i&0&0\\-i&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&1&0\\0&0&0&0\\1&0&0&0\\0&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&i&0\\0&0&0&0\\-i&0&0&0\\0&0&0&0\end{pmatrix},$$
$$\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&i\\0&0&-i&0\\0&-i&0&0\\-i&0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&0\\0&0&0&1\\0&0&0&0\\0&1&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&0\\0&0&0&i\\0&0&0&0\\0&-i&0&0\end{pmatrix}, \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}, \begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&i\\0&0&-i&0\end{pmatrix}.$$

Finally, let us give a proof of Theorem III.3.

Proof. For $k \in \{2r-1,\ldots,2(n-r)-1\}$, define $A_k, A'_k \in M(\gamma(n,k),r,\mathbb{R})$ by setting $(A_k)_{jl} = (A'_k)_{jl} = x_{l+1}^j$ for all $j \in \{0,\ldots,\gamma(n,k)-1\}, l \in \{0,\ldots,r-1\}$. Observe that both A_k and A'_k can be considered as the first r columns of a $\gamma(n,k)\times\gamma(n,k)$ Vandermonde matrix and since $x_j \neq x_l$ for all $j,l \in \{1,\ldots,r\}$ with $j \neq l$ and $x_l \neq 0$ for all $l \in \{1,\ldots,r\}$ they are thus totally non-singular. Applying Theorem V.3 to A_k, A'_k then concludes the proof. □

B. Proof of Theorem III.1

Let us now give a proof of Theorem III.1.

[14] The minors of a $m \times 1$ matrix are simply the entries of the matrix.

Proof. Define $Y_k, X_k \in H(n),\ k \in \{1,\dots,2n-3\}$, by

$$(X_k)_{jl} := \delta_{j+l,k} \cos\left(\frac{j-l}{2n}\pi\right),$$
$$(Y_k)_{jl} := i\delta_{j+l,k} \sin\left(\frac{j-l}{2n}\pi\right),$$
$$j,l \in \{0,\dots,n-1\}.$$

Next observe two things:

1. The matrices $\{X_1, Y_1, \dots, X_{2n-3}, Y_{2n-3}\} \subseteq H(n)$ are linearly independent by equations (9) and (10).

2. Since $0 < \frac{j-l}{2n}\pi < \frac{\pi}{2}$ for $j,l \in \{0,\dots,n-1\}$, $j > l$, we find $(X_k)_{jl} \neq 0$ and $(Y_k)_{jl} \neq 0$ for $j + l = k$, $j > l$.

Let $u_k, w_k \in \mathbb{R}^{\gamma(n,k)},\ k \in \{1,\dots,2n-3\}$, be such that $\iota_k(u_k) = X_k - \delta_{k/2,\lceil k/2\rceil} e_{\lceil k/2\rceil} e^*_{\lceil k/2\rceil}$, $\iota_k(iw_k) = Y_k$ and note that both u_k and w_k have no vanishing entry. Thus, by Corollary V.4, $\tilde{G} := (e_0e_0^*, \dots, e_{n-1}e_{n-1}^*) \cup (X_1, Y_1, \dots, X_{2n-3}, Y_{2n-3})$ is 1-complete.

Let $G := (e_0e_0^*, \dots, e_{n-1}e_{n-1}^*, v_1v_1^*, \overline{v}_1\overline{v}_1^*, \dots, v_{2n-3}v_{2n-3}^*, \overline{v}_{2n-3}\overline{v}_{2n-3}^*)$. To conclude the proof, we show that $\mathrm{Span}(G) = \mathrm{Span}(\tilde{G})$. First note that for $k \in \{1,\dots,2n-3\}$

$$v_kv_k^* = \sum_{j=1}^{2n-3} x_k^j(X_j + Y_j) + e_0e_0^* + x_k^{2n-2} e_{n-1}e_{n-1}^*,$$
$$\overline{v}_k\overline{v}_k^* = \sum_{j=1}^{2n-3} x_k^j(X_j - Y_j) + e_0e_0^* + x_k^{2n-2} e_{n-1}e_{n-1}^*$$

and thus $\mathrm{Span}(G) \subseteq \mathrm{Span}(\tilde{G})$. In order to show that $\mathrm{Span}(\tilde{G}) \subseteq \mathrm{Span}(G)$, consider the matrix

$$T := \begin{pmatrix} x_1 & x_1^2 & x_1^3 & \dots & x_1^{2n-3} \\ x_2 & x_2^2 & x_2^3 & \dots & x_2^{2n-3} \\ x_3 & x_3^2 & x_3^3 & \dots & x_3^{2n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ x_{2n-3} & x_{2n-3}^2 & x_{2n-3}^3 & \dots & x_{2n-3}^{2n-3}. \end{pmatrix}$$

The matrix T is a Vandermonde matrix and thus invertible if $x_i \neq x_j$ for $i \neq j$. Hence we find [15]

$$X_k = \frac{1}{2}\sum_{j=1}^{2n-3} (T^{-1})_{kj}(v_jv_j^* + \overline{v}_j\overline{v}_j^* - 2e_0e_0^* - 2x_k^{2n-2} e_{n-1}e_{n-1}^*),$$
$$Y_k = \frac{1}{2}\sum_{j=1}^{2n-3} (T^{-1})_{kj}(v_jv_j^* - \overline{v}_j\overline{v}_j^*)$$

[15] Different from the rest of the present paper, the indices we use to label T begin with 1, not with G.

and this shows that $\mathrm{Span}(\tilde{G}) \subseteq \mathrm{Span}(G)$. □

Remark Note that there are many possible choices for the phases of the v_i. The only constraint is that $j\varphi \neq \frac{k\pi}{2}$ for all $j \in \{1, \ldots, n-1\},\ k \in \mathbb{Z}$.

C. Proof of Theorem IV.1 and Proposition IV.2

For $X_r \in \mathcal{S}_r^n$, $E \in H(n)$, $\epsilon \geq 0$ and a measurement M define the set

$$F_\epsilon(X_r, E, M) := \{Y \in \mathcal{S}^n : \|M(Y) - b\|_2 \leq \epsilon\}, \tag{16}$$

where $b = M(X_r + E)$.

Lemma V.5. *(Stability.) Let M be an r-complete measurement and let $\epsilon > 0$. Then, there exists a constant $C_M > 0$ independent of ϵ such that for all $X_r \in \mathcal{S}_r^n$, and $E \in H(n)$ with $\|M(E)\|_2 \leq \epsilon$ we have*

$$Y \in F_\epsilon(X_r, E, M) \Rightarrow \|Y - X_r\|_2 \leq C_M \epsilon.$$

Proof. Denote by $\pi : H(n) \to \mathrm{Range}(M^*)$ the orthogonal projection on the subspace $\mathrm{Range}(M^*) \subseteq H(n)$ and by $\pi^\perp : H(n) \to \mathrm{Ker}(M)$ the orthogonal projection on the subspace $\mathrm{Ker}(M) \subseteq H(n)$. Furthermore, let $Y' := \pi^\perp(X_r) + \pi(Y)$ and let σ_{min} be the smallest singular value of M [16]. Then, we find

$$\begin{aligned}
\|X_r - Y'\| = \|\pi(X_r - Y)\|_2 &\leq \frac{1}{\sigma_{min}} \|M(Y - X_r)\|_2 \\
&\leq \frac{1}{\sigma_{min}} (\|M(X_r) - b\|_2 + \|M(Y) - b\|_2) \leq \frac{1}{\sigma_{min}} (\|M(E)\|_2 + \epsilon) \\
&\leq \frac{2}{\sigma_{min}} \epsilon.
\end{aligned} \tag{17}$$

From the spectral variation bound for Hermitian matrices (Theorem III.2.8 of [29]) we conclude that

$$\begin{aligned}
\|\mathrm{Eig}(X_r) - \mathrm{Eig}(Y')\|_2 &= \sqrt{\sum_{i=1}^{r} \left(\lambda_i(X_r) - \lambda_i(Y')\right)^2 + \sum_{i=r+1}^{n} \lambda_i(Y')^2} \\
&\leq \frac{2}{\sigma_{min}} \epsilon.
\end{aligned}$$

But this implies that $|\lambda_i(Y')| \leq \frac{2}{\sigma_{min}} \epsilon$ for $i \in \{r+1, \ldots, n\}$.

Next, note that

$$\kappa := - \max_{Z \in \mathrm{Ker}(M), \|Z\|_2 = 1} \lambda_{n-r}(Z)$$

[16] We assume M to have full rank.

exists by compactness of $\{Z \in \mathrm{Ker}(M) : \|Z\|_2 = 1\}$ and continuity of λ_{n-r}. Furthermore, by Proposition II.2, every nonzero $Z \in \mathrm{Ker}(M)$ has at least $r+1$ negative eigenvalues and hence we conclude that $\kappa > 0$.

There exists $Z \in \mathrm{Ker}(M)$ with $\|Z\|_2 = 1$ and $\alpha \geq 0$ such that $Y = Y' + \alpha Z$ [17]. Since $Y \geq 0$ we conclude from Weyl's inequality (Theorem III.2.1 of [29]) that

$$0 \leq \lambda_n(Y' + \alpha Z) \leq \lambda_{r+1}(Y') + \alpha \lambda_{n-r}(Z) \leq \frac{2}{\sigma_{min}}\epsilon - \alpha\kappa.$$

and hence we find

$$\alpha \leq \frac{2}{\kappa \sigma_{min}}\epsilon. \tag{18}$$

Finally, combining equations (17) and (18), we conclude that

$$\begin{aligned}\|Y - X_r\|_2 = \|Y' + \alpha Z - X_r\|_2 &\leq \|Y' - X_r\|_2 + \|\alpha Z\|_2 \\ &\leq \left(\frac{2}{\sigma_{min}} + \frac{2}{\kappa\sigma_{min}}\right)\epsilon.\end{aligned}$$

Choosing $C_M = \frac{2}{\sigma_{min}}(1 + \frac{1}{\kappa})$ then proves the claim. □

Remark Since κ just depends on $\mathrm{Ker}(M)$, it is independent of the choice of basis for $\mathrm{Range}(M^*)$. Thus, since it is always possible to choose an orthonormal basis of $\mathrm{Range}(M^*)$, the constant C_M is mainly determined by κ.

The proof of Theorem IV.1 is an immediate consequence of this lemma.

Remark Let M be a measurement that is not r-complete. Then there exist $Z_r \in \mathcal{S}_r^n$ and $Z \in \mathcal{S}^n$ with $Z_r \neq Z$ such that $M(Z_r - Z) = 0$ and we find $Z \in F_\epsilon(Z_r, E, M)$ for all $\epsilon > 0$ and $E \in H(n)$ with $\|M(E)\|_2 \leq \epsilon$. Thus, if $\mathbb{1} \in \mathrm{Range}(M^*)$, the r-complete property is necessary to enable the recovery of every $X_r \in \mathcal{S}_r^n$ via the optimization problem (5).

Finally let us give the proof of Proposition IV.2.

Proof. From Theorem IV.1 we obtain the bound $\|Y - xx^*\|_2 \leq C_M\epsilon$ and the proof of Lemma IV yields the bound $\sqrt{\sum_{i=2}^n \lambda_i(Y)^2} \leq C_M\epsilon$. From this we find

$$\|xx^* - \hat{x}\hat{x}^*\|_2 \leq \|Y - xx^*\|_2 + \|Y - \hat{x}\hat{x}^*\|_2 \leq 2C_M\epsilon.$$

[17] Note that $\alpha Z = \pi^\perp(Y) - \pi^\perp(X_r) \in \mathrm{Ker}(M)$.

Finally let $\varphi \in [0, 2\pi)$ be such that $\langle x, e^{i\varphi}\hat{x}\rangle$ is positive. Then,

$$\begin{aligned}
\|x - e^{i\varphi}\hat{x}\|_2^2\|x\|_2^2 &= \left(\|x\|_2^2 + \|\hat{x}\|_2^2 - 2\mathrm{Re}\left(\langle x, e^{i\varphi}\hat{x}\rangle\right)\right)\|x\|_2^2 \\
&= \left(\|x\|_2^2 + \|\hat{x}\|_2^2 - 2|\langle x, \hat{x}\rangle|\right)\|x\|_2^2 \\
&\leq \left(\|x\|_2^2 + \|\hat{x}\|_2^2 - 2|\langle x, \hat{x}\rangle|\right)\left(\|x\|_2^2 + \|\hat{x}\|_2^2 + 2|\langle x, \hat{x}\rangle|\right) \\
&= \left(\|x\|_2^2 + \|\hat{x}\|_2^2\right)^2 - 4|\langle x, \hat{x}\rangle|^2 \\
&= \|x\|_2^4 + \|\hat{x}\|_2^4 - 2|\langle x, \hat{x}\rangle|^2 + 2\|x\|_2^2\|\hat{x}\|_2^2 - 2|\langle x, \hat{x}\rangle|^2 \\
&\leq 2\left(\|x\|_2^4 + \|\hat{x}\|_2^4 - 2|\langle x, \hat{x}\rangle|^2\right) \\
&= 2\|xx^* - \hat{x}\hat{x}^*\|_2^2 \\
&\leq 2(2C_M\epsilon)^2.
\end{aligned}$$

□

---

[1] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Applied and Computational Harmonic Analysis*, 20(3):345–356, 2006.

[2] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. *Applied and Computational Harmonic Analysis*, 2014.

[3] Michael Kech and Michael M. Wolf. Quantum tomography of semi-algebraic sets with constrained measurements. *arXiv:1507.00903*, 2015.

[4] Damien Mondragon and Vladislav Voroninski. Determination of all pure quantum states from a minimal number of observables. *arXiv preprint arXiv:1306.1214*, 2013.

[5] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. How many orthonormal bases are needed to distinguish all pure quantum states? *arXiv preprint arXiv:1504.01590*, 2015.

[6] Teiko Heinosaari, Luca Mazzarella, and Michael M Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318(2):355–374, 2013.

[7] Matthew Fickus, Dustin G Mixon, Aaron A Nelson, and Yang Wang. Phase retrieval from very few measurements. *Linear Algebra and its Applications*, 449:475–499, 2014.

[8] Radu Balan, Bernhard G Bodmann, Peter G Casazza, and Dan Edidin. Painless reconstruction from magnitudes of frame coefficients. *Journal of Fourier Analysis and Applications*, 15(4):488–501, 2009.

[9] Boris Alexeev, Afonso S Bandeira, Matthew Fickus, and Dustin G Mixon. Phase retrieval with polarization. *SIAM Journal on Imaging Sciences*, 7(1):35–66, 2014.

[10] Afonso S Bandeira, Yutong Chen, and Dustin G Mixon. Phase retrieval from power spectra of masked signals. *Information and Inference*, page iau002, 2014.

[11] Emmanuel J Candes, Yonina C Eldar, Thomas Strohmer, and Vladislav Voroninski. Phase retrieval via matrix completion. *SIAM Review*, 57(2):225–251, 2015.

[12] Emmanuel J Candes, Thomas Strohmer, and Vladislav Voroninski. Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming. *Communications on Pure and Applied Mathematics*, 66(8):1241–1274, 2013.

[13] Emmanuel J Candes and Xiaodong Li. Solving quadratic equations via phaselift when there are about as many equations as unknowns. *Foundations of Computational Mathematics*, 14(5):1017–1026, 2014.

[14] Emmanuel J Candes, Xiaodong Li, and Mahdi Soltanolkotabi. Phase retrieval via wirtinger flow: Theory and algorithms. *IEEE Transactions on Information Theory*, 61(4):1985–2007, 2015.

[15] David Gross, Felix Krahmer, and Richard Kueng. A partial derandomization of phaselift using spherical designs. *Journal of Fourier Analysis and Applications*, 21(2):229–266, 2015.

[16] Richard Kueng, David Gross, and Felix Krahmer. Spherical designs as a tool for derandomization: The case of phaselift. In *11th international conference on Sampling Theory and Applications (SampTA 2015), Washington, USA*, 2015.

[17] Bernhard G Bodmann and Nathaniel Hammen. Stable phase retrieval with low-redundancy frames. *Advances in computational mathematics*, 41(2):317–331, 2015.

[18] Bernhard G Bodmann and Nathaniel Hammen. Algorithms and error bounds for noisy phase retrieval with low-redundancy frames. *Applied and Computational Harmonic Analysis*, 2016.

[19] Jianxin Chen, Hillary Dawkins, Zhengfeng Ji, Nathaniel Johnston, David Kribs, Frederic Shultz, and Bei Zeng. Uniqueness of quantum states compatible with given measurement results. *Physical Review A*, 88(1):012109, 2013.

[20] Emmanuel J Candès and Benjamin Recht. Exact matrix completion via convex optimization. *Foundations of Computational mathematics*, 9(6):717–772, 2009.

[21] Emmanuel J Candes and Yaniv Plan. Matrix completion with noise. *Proceedings of the IEEE*, 98(6):925–936, 2010.

[22] Emmanuel J Candès and Terence Tao. The power of convex relaxation: Near-optimal matrix completion. *Information Theory, IEEE Transactions on*, 56(5):2053–2080, 2010.

[23] Benjamin Recht, Maryam Fazel, and Pablo A Parrilo. Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization. *SIAM review*, 52(3):471–501, 2010.

[24] David Gross, Yi-Kai Liu, Steven T Flammia, Stephen Becker, and Jens Eisert. Quantum state tomography via compressed sensing. *Physical review letters*, 105(15):150401, 2010.

[25] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. Tasks and premises in quantum state determination. *Journal of Physics A: Mathematical and Theoretical*, 47(7):075302, 2014.

[26] Toby Cubitt, Ashley Montanaro, and Andreas Winter. On the dimension of subspaces with bounded schmidt rank. *Journal of Mathematical Physics*, 49(2):022107, 2008.

[27] Michael Kech, Péter Vrana, and Michael Wolf. The role of topology in quantum tomography. *Journal of Physics A: Mathematical and Theoretical*, 48(26):265303, 2015.

[28] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

[29] Rajendra Bhatia. *Matrix analysis*, volume 169. Springer Science & Business Media, 2013.